REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-8 are currently pending in the application; Claims 1, 4, and 5 having been amended; and new Claims 6-8 having been added by the present amendment. No new matter is added.

By way of summary, the Official Action presents the following issues: Claims 1-5 were rejected under 35 U.S.C. § 112, second paragraph, as indefinite; and Claims 1-5 were rejected under 35 U.S.C. § 103(a) as unpatentable over Moline (U.S. Patent No. 5,883,957, hereinafter Moline) in view of Scott (U.S. Patent No. 5,987,123, hereinafter Scott).

The undersigned acknowledges with appreciation the courtesy extended to Applicant's representatives by Examiner LaForgia by holding a person interview with the undersigned on April 8, 2004. In the interview, proposed claim changes were discussed, and Applicant's invention was explained in light of the proposed claim changes. No agreement was reached during the interview, pending the formal submission of a response to the outstanding Official Action.

With respect to the rejection of Claims 1-5 under 35 U.S.C. § 112, second paragraph, Applicants respectfully traverse this rejection.

The Official Action states that Applicants fail to adequately define the phrases "management information" and "calculation information." However, the specification clearly delineates parameters that relate to the management of the digital data, and parameters that are used in calculations to assist in managing the digital data.[1] MPEP § 2173.01 is quite clear that an applicant may be their own lexicographer provided the terms they choose are not used in ways that are contrary to the accepted meanings in the art. Such is the case with the

[1] Specification at page 37.

present claimed terms found objectionable in the outstanding Office Action as will be explained below. It should be noted that the breadth of a claim is not to be equated with its indefiniteness. Despite the specific examples of the terms "management information," and "calculation information" cited below, these generic claim terms have been adopted to give a broader meaning than any of the specific instances cited below (MPEP § 2173.04).

With respect to "management information" the specification describes various parameters that relate to the stored digital media and are used to manage the digital file. Specifically, parameters stored in relation to the digital content include a content identifier, the number of reproducing operations, the reproduction limit, the content title, the artist's name, content key, and a message authentication code (MAC) value.[2] Moreover, the phrase "management information" describes information that might include, but is not limited to, a set of the abovementioned parameters.

The phrase "calculation information" refers to a subset of parameters from the above-mentioned "management information," some of which are updateable based on the status of the digital file. The subset of parameters making up the "calculation information" is combined with encryption key data to generate a MAC value which is used to help manage the digital data. "Calculation information" may include, but is not limited to parameters such as content identifier, number of reproducing operations performed, production limit, etc.

Accordingly, since "management information" and "calculation information" are adequately defined in the specification and the terms are not repugnant to their ordinary meaning, Applicant requests that the rejection of Claims 1-5 under 35 U.S.C. § 112, second paragraph, be withdrawn.

The Official Action has rejected Claims 1-5 under 35 U.S.C. § 103(a) as unpatentable over Moline in view of Scott. The Official Action cites Moline as disclosing the Applicant's

[2] Specification at page 37.

invention with the exception of comparing calculation results and controlling access to digital content based on that comparison. The Official Action cites Scott as curing the deficiencies of Moline. Applicants respectfully traverse this rejection.

The present inventors identified a system and method that prevents data from being tampered with or copied in an authorized manner. In an exemplary embodiment of the present invention, encrypted digital data is downloaded with management information which includes various parameters relating to the downloaded data. Among other parameters, the management information also includes usage rule parameters restricting the transfer and use of the digital data. The usage restrictions include limits on how many times the data can be copied, how many times the data can be transferred, etc.[3] These parameters form the basis for a calculated MAC value generated each time an "operation" is performed on the digital media. Operations may include playing, recording, or transferring the digital data from one device to another (checked-in or checked-out).[4]

The MAC value is generated using the encryption key for the content device, as well as other possibly updatable calculation information which reflect the current status of the digital data.[5] Each time an operation is initiated on the digital file, the MAC value which is currently stored in memory is compared to a newly calculated MAC value which is generated in response the initiation of the operation. If the result of the comparison shows that the two MAC values differ, then the content of the digital file has been altered or the contents have been tampered with.[6] If tampering is detected then the use of the digital data is restricted.

Amended Claim 1 recites, *inter alia*, an information processing apparatus comprising:

> "... holding means for holding management information associated with said content data stored in said storage means,

[3] Specification at pages 8-9.
[4] Specification at page 37.
[5] Specification at page 37, lines 15-21.
[6] Specification at Fig. 6.

> wherein said management information includes calculation information;
>
> calculation means for performing a predetermined calculation on the basis of said encryption key and said calculation information, said calculation information including updatable information which is updated upon execution of a predetermined operation performed on said content data ...
>
> control means for comparing the result of the calculation performed by said calculation means with a previous calculation result stored in said memory means and controlling use of said content data stored in said storage means in accordance with the result of the comparison."

Claim 1 was amended to emphasize that the calculation information is updated upon an execution of a predetermined operation performed on the content data. Moline describes that an encrypted MIDI file can be downloaded by a user and decrypted using an appropriate decryption key.[7] Moline's device processes an encrypted MIDI track with a decryption key and generates an unencrypted MIDI file, which the user of the device can then play. The decryption mechanism in Moline's device (1325) can decrypt MIDI tracks or files from several sources by maintaining a keyless data structure (1503) in which there is an entry (1505) for each source. Moline's device determines which key is to be used to decrypt a given file or track by means of a source specifier (1501) which may be part of a header received with the MIDI track or file.[8]

Scott describes a method of validating incoming files by checking the files against a two-level security system that determines the validity of their source. Digital affidavits identifying the source of each received file are checked against a list of acceptable sources that the user and the system have deemed trustworthy. If the data is determined to be from a trustworthy source then the data is accepted by the device.[9]

The requirements for a *prima facie* case of obviousness are (1) there must be some suggestion or motivation in the references themselves or in the knowledge generally available

[7] Moline at column 2, lines 45-57.
[8] Moline at column 20, line 59-column 21, line 13.
[9] Scott at column 1, lines 40-60.

to one of ordinary skill in the art to modify the reference or to combine the reference teachings, (2) there must be a reasonable expectation of success, and (3) the prior art reference must teach or suggest all of the claim limitations. It is respectfully submitted that the outstanding Office Action fails to make a *prima facie* case of obviousness, because there is no suggestion or motivation to modify Moline with Scott, and Moline and/or Scott even if combined, fail to teach all of the limitations of the claimed invention.

The Official Action admits that Moline does not teach a control means for comparing the result of the calculation performed by said calculation means with a previous calculation result stored in said memory means and controlling use of said content data stored in said storage means in accordance with the result of the comparison. To cure the deficiency of Moline the Official Action turns to Scott.

Regarding lack of motivation, Moline describes a method for downloading digital data and decrypting the data using a locally stored decryption algorithm, while Scott describes a method for filtering data sent from undesirable, or unknown, sources. Moline's device includes a list of sources from which each of the files is obtained, and that the user is the party initiating the connection to the source via a network.[10] Therefore, Moline's system is suited to allow the user to initiate reception of received data from source with which the user initiated the connection. There is no discussion of filtering data from unwanted sources, or even receiving data from a source that might be questionable. Thus, there is no motivation whatsoever to incorporate a security mechanism that serves to filter data from unwanted sources, as described by Scott, into Moline's system. Therefore, there is no motivation to add Scott's method of filtering data received from unknown sources with Moline's method for downloading and decrypting digital MIDI files.

[10] Moline at column 21, lines 5-12.

Even if Moline and Scott were combined, the combination fails to teach all of the limitations recited in amended Claim 1.

The Official Action states that Moline teaches a calculation means for performing a predetermined calculation on the basis of an encryption key and calculation information, the calculation information including updatable information which is updated with operation of said content data. At no point does Moline disclose or suggest performing a calculation on the basis of an encryption key and calculation information. Furthermore, there is no information in Moline, which could be described as being "updated with an operation of [the] content data" as recited in amended Claim1.

The portion of Moline cited in the Official Action describes a method for storing encryption keys from various sources so that MIDI files received from those sources can be successfully decrypted.[11] However, none of the parameters stored in Moline's device are updated upon the operation of the data and no calculation is performed using any encryption information and calculation data, as recited in amended Claim 1. The only function being performed in Moline is the use of a decryption key to decrypt a received MIDI file.

Furthermore, in the interview, Examiner LaForgia stated that a portion of Moline, not cited in the official action, might disclose the limitations recited in amended Claim 1.[12] This portion of Moline describes a method of developing a relationship between a key and a decrypting synthesizer, and ensuring that the user (person downloading the data) is able to receive a key that is applicable, or able to decrypt, the downloaded data. Specifically, Moline describes that keys may be associated with given sites, users, or specific executions, and based on these associations; a decryption key may be downloaded together with the digital content. In contrast, amended Claim 1 recites performing a predetermined calculation on the basis of an encryption key and updatable calculation information, which is updated upon the

[11] Moline at column 20, line 59-column 21, line 13.
[12] Moline at column 21, lines 40-57.

execution of a predetermined operation performed on said content data. At no point does Moline discuss any updatable calculation information, or that a predetermined calculation is performed based on this updated calculation, as recited in amended Claim 1. There are no updatable parameters discussed in Moline's disclosure. In contrast, Moline only discusses the transfer of keys, and does not describe that any calculations are performed on the basis of a value that is updated as a function of an operation performed on the content data.

The Official Action relies on Scott to describe control means for comparing the result of the calculation performed by the calculation means with a previous calculation result stored in the memory means and controlling the use of the content data stored in the storage means in accordance with the result of the comparison. However, Scott does not compare a calculation result with a previous calculation result. To the contrary, Scott describes comparing a received checksum value (indicative of the source of data) with a checksum value previously stored in the user's device. Based on this comparison, the system determines if the source of the received file is on the list of reliable sources. There is no comparison of newly calculated and previously calculated results in Scott's device.

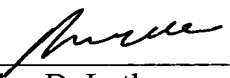
Therefore, neither Moline nor Scott individually or in combination teach or disclose all of the elements of the claimed invention. Accordingly, Applicants request the rejection of Claims 1-5 under 35 U.S.C. § 103 be withdrawn.

Claims 6-8 are drafted to avoid an interpretation under 35 U.S.C. § 112 ¶ 6, but are nevertheless believed to patentable define over the asserted prior art for similar reasons given above with regard to amended Claim 1.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1-8 is definite and patentably distinguishing over the prior art. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/03)

BDL/ATH/la
I:\ATTY\ATH\PROSECUTION\20'S\203742-US\203742 AM.DOC